あるテータ関数の積の q 展開係数と合同数との関係

大塲 彦浄

平成21 年2 月27 日

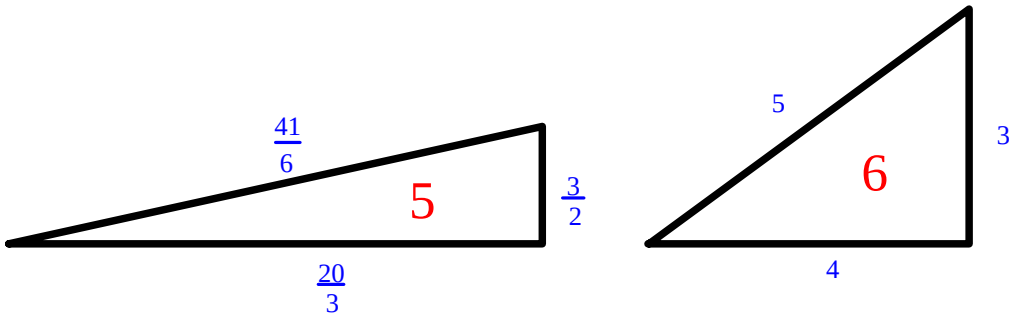
目 次

1 Introduction

本修士論文は Tunnell による論文 [16] の総合報告である. この論文では合同数問題といわれる問題にほぼ解を与えている Tunnell の定理が示されている. しかし, 未解決の弱 BSD 予想が絡んでいるため完全に解決されたとは言えないことを注意しておく. このことについては後に触れる.

定義 1.1 (**合同数**)**.** 平方因子を持たない自然数 n が**合同数**であるとは, n が有理数の 3 辺を持つ直角三角形の面積になるときにいう.

例 1.2. $5, 6$ は合同数である.



ここで問題となるのは以下である.

問題 1.3. 与えられた平方因子を持たない自然数がどのような条件のとき合同数となりうるか ?

一般にこの問題を考えることは難しい. なぜならば, n を平方因子を持たない自然数としたとき関係式

$$X^2 + Y^2 = Z^2, \quad \frac{XY}{2} = n$$

が有理数解 (X, Y, Z) を持つならば n は合同数であることがわかるが, この様な有理数の組 (X, Y, Z) の可能性は無限通り存在するからである. この合同数問題に関連して Tunnell [16] は以下のような定理を結果として与えた.

定理 1.4 (**Tunnell**)**.** n を平方因子を持たない自然数とする. n が合同数ならば次が成り立つ.

n が奇数のとき

$$\#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\}.$$

n が偶数のとき

$$\#\{x,y,z\in\mathbb{Z}|\frac{n}{2}=4x^2+y^2+32z^2\}=\frac{1}{2}\#\{x,y,z\in\mathbb{Z}|\frac{n}{2}=4x^2+y^2+8z^2\}.$$

注目すべき点はこの方程式の整数解の個数は有限回の操作で求められる点である. この逆は弱 BSD 予想を認めれば成立する. つまり, 弱 BSD 予想を認めれば n に対して上で定められた方程式の解の個数を数えることにより, n が合同数であるかどうかを判定することができる. 一見すると初等的な問題であるが証明を述べるには楕円曲線, モジュラー形式などの理論が必要となる. これらについて以後の章で基本事項をまとめていく.

簡単のため, n が奇数の場合に Tunnell が示したことを述べる. 方程式の解の個数

$$\#\{x,y,z\in\mathbb{Z}|n=2x^2+y^2+32z^2\}-\frac{1}{2}\#\{x,y,z\in\mathbb{Z}|n=2x^2+y^2+8z^2\} \tag{1.5}$$

を求めることは, テータ関数の積 $g(z)\theta_2(z)$ の q 展開の n 番目の係数を求めることに対応している. Tunnell の主定理を述べる.

$z\in\mathbb{C}$ $(\mathrm{Im}\ z>0), q=e^{2\pi iz},\ t\in\mathbb{Z}_{>0}$ とし,

$$g(z)=q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n}),\quad \theta_t(z)=\sum_{n=-\infty}^{\infty}q^{tn^2}.$$

とする. $g(z)\theta_2(z)$ の q 展開を次のようにおく.

$$g(z)\theta_2(z)=\sum_{n=1}^{\infty}a(n)q^n.$$

この状況の下, Tunnell は次を示した.

定理 1.6 (Tunnell [16]). n を平方因子を持たない奇数とする. このとき,

$$L(E_n,1)=\frac{a(n)^2\beta n^{-\frac{1}{2}}}{4}.$$

ただし, $\beta=\displaystyle\int_1^{\infty}\frac{dx}{\sqrt{x^3-x}}=2.62205\cdots$ である.

証明の概略を簡単に述べることにする. ある平方因子を持たない奇数の自然数 n が合同数であることと楕円曲線

$$E_n: y^2=x^3-n^2x$$

のランクは 0 より大きくなることが同値であることが初等的な証明により導かれる. また, ランクが 0 より大きいならば Coates-Wiles [3] の結果により楕円曲線 E_n の L

関数の $s=1$ での値が 0 であることがわかる. また,

弱 BSD 予想　E を有理数体 $\mathbb{Q}$ 上の楕円曲線とする. このとき,

$$\mathrm{ord}_{s=1}L(E,s) = \mathrm{rank}\ E(\mathbb{Q}).$$

を認めれば, $L(E_n,1)=0$ ならば $\mathrm{rank}\ E_n(\mathbb{Q})>0$ であることがわかる.

E_n の L 関数は E_1 の L 関数の指標 $\chi_n(*)=\left(\frac{n}{*}\right)$ (ヤコビ記号) によるツイストで書ける. つまり,

$$L(E_n,s) := \sum_{m=1}^{\infty}\frac{b_{m,n}}{m^s}$$

とおいたとき,

$$L(E_n,s) = L(E_1,\chi_n,s) := \sum_{m=1}^{\infty}\frac{\chi_n(m)b_{m,1}}{m^s}$$

と書ける.

また,

$$L(E_1,s) = \sum_{m=1}^{\infty}\frac{b_{m,1}}{m^s}$$

に対して

$$f_{E_1}(z) := \sum_{m=1}^{\infty} b_{m,1}q^m$$

とおけば, f_{E_1} は重さ 2 の保型形式となることが Weil の定理より示される [4, p.142]. ここで注目すべき関係として

$$L(E_1,\chi_n,s) = L(f_{E_1},\chi_n,s) = L(E_n,s)$$

がある. つまり, E_n の L 関数の $s=1$ での値を調べるには保型形式 f_{E_1} の L 関数の $s=1$ での値を調べればよい.

次は L 関数の特殊値と保型形式との関係について述べる. 志村対応という重さ 3/2 と重さ 2 の保型形式との間に対応が与えられ, Waldspurger [17] より重さ 2 の保型形式 ϕ に対応する L 関数の $s=1$ での値は**定数と志村対応により ϕ に写る重さ 3/2 の保型形式のある線形結合があり, その q 展開係数の平方**の積に等しいことが示された. Tunnell は楕円曲線 E_n に対してこの結果を応用した. Tunnell は重さ 2 の保型形式として f_{E_1} をとり, (志村対応は一対一ではないが) 志村対応により f_{E_1} に写る重さ 3/2 の保型形式が $g(z)\theta_2(z)$ であることを示した. Waldspurger [17] の結果より E_n の L 関数の $s=1$ の値はテータ関数の積 $g(z)\theta_2(z)$ の q 展開係数 $a(n)$ の 2 乗と定数との積で書き表せることがわかる. よって, n が合同数ならば $a(n)=0$ であり, 弱 BSD 予想を認めれば, $a(n)=0$ のとき n は合同数であることがわかる. $g(z)\theta_2(z)$ の n 番目の係数が (1.5) となることは最後の章で述べる.

謝辞

本修士論文を書くに至るまで親切に御指導下さった雪江明彦先生に感謝します. また, 同じセミナーの仲間であった加藤成美氏, 田嶋和明氏, 高橋雄氏, 伊藤高志氏に感謝します.

2　楕円曲線と保型形式

2.1　楕円曲線

ここでは, 楕円曲線の一般論について簡単に復習することにする. k を体とする. k 有理点を持つ種数 1 の非特異な射影曲線を k 上の**楕円曲線**という. この曲線を E とすると, E は Weierstrass 方程式といわれる次の曲線で表せる. また, $O = (0, 1, 0)$ を無限遠点という.

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2.1}$$

ここで, $a_1, a_2, a_3, a_4, a_6 \in k$ である. E が方程式 (2.1) で定まる楕円曲線のとき,

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned}$$

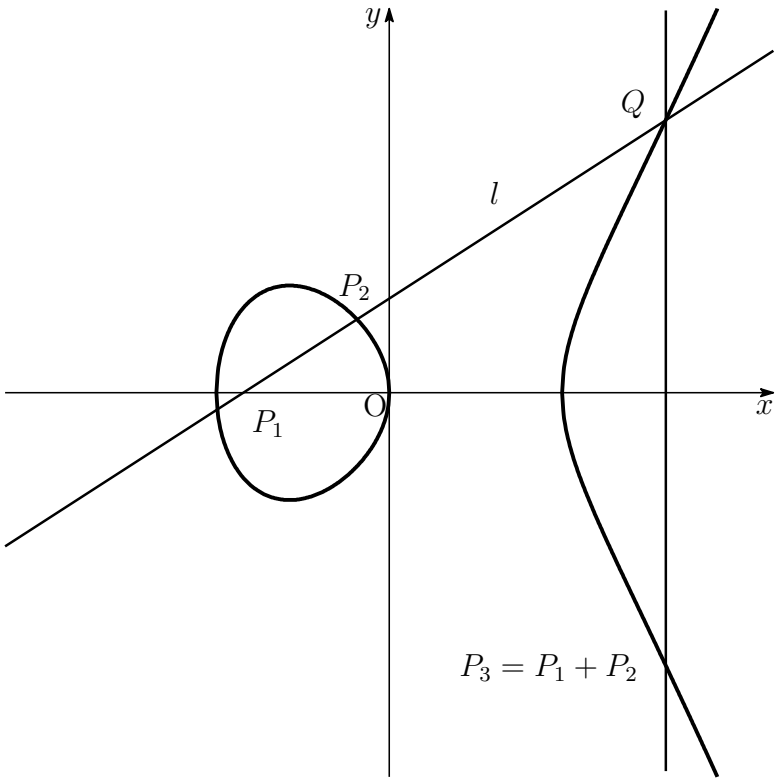
とおく. Δ を E の判別式と呼ぶ. $\Delta \neq 0$ のとき E は非特異となり, 楕円曲線となる. よって楕円曲線とは Weierstrass 方程式 (2.1) で定まり $\Delta \neq 0$ となる曲線のことと考えてよい. k の標数が $2, 3$ と異なるとき Weierstrass 方程式として次がとれる.

$$y^2 = x^3 + ax + b.$$

このとき $\Delta = -2^4(4a^3 + 27b^2)$ となる. 以降 K を代数体とする. E を K 上定義された楕円曲線とし, $E(K)$ を次のようにおく.

$$E(K) := \{(X, Y, Z) \in \mathbb{P}^2(K) | Y^2Z = X^3 + aXY^2 + bZ^3\}.$$

E 上の 2 点 P_1, P_2 に対し P_1 と P_2 を通る直線を l とする. l と E の 3 つ目の交点を Q とおく. Q の x 軸対称の点 P_3 を $P_1 + P_2$ と定義する.



この演算により $E(K)$ にはアーベル群の構造が入ることが知られている [14, p.55]. また, 次の定理が知られている.

定理 2.2 (**Mordell-Weil の定理, [14, p.189]**). $E(K)$ は有限生成アーベル群である. つまり $E(K)$ は

$$E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$$

と書ける. ここで $E(K)_{\mathrm{tors}}$ は有限アーベル群である. r を楕円曲線 E のランクという.

この定理は有理数体 $\mathbb{Q}$ の場合は Mordell により示され [14, p.201], 一般の代数体上のアーベル多様体の場合は Weil により示された.

2.2 整数重さの保型形式

ここでは, 保型形式とカスプ形式の一般論を解説する. まず, 特殊線形群 $SL_2(\mathbb{Z})$ と複素上半平面 $\mathbb{H}$ を

$$SL_2(\mathbb{Z}) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z}, \det\gamma = 1 \right\},$$
$$\mathbb{H} := \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$$

と定める. また $SL_2(\mathbb{Z})$ の $\mathbb{H}$ への作用を次の様に

$$z \in \mathbb{H}, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \quad \text{に対して} \quad \gamma z = \frac{az+b}{cz+d}$$

と一次分数変換で定める.

今後話を進める上で重要となる $SL_2(\mathbb{Z})$ の部分群 Γ_0, Γ_1 を

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \mod N \right\},$$
$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \middle| a \equiv 1 \mod N \right\}$$

と定義する. $\Gamma_1(N)$ は $\Gamma_0(N)$ の正規部分群でありその剰余群は $(\mathbb{Z}/N\mathbb{Z})^*$ と同型である. また $\Gamma(N)$ を

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

とおき, $SL_2(\mathbb{Z})$ の部分群 Γ で $\Gamma \supset \Gamma(N)$ となるとき Γ をレベル N の合同部分群と呼ぶ.

ここで, $\mathbb{H}/\Gamma_0(N)$ は楕円曲線 E と E 上の位数 N の点の組の同値類に対応しており, $\mathbb{H}/\Gamma(N)$ は楕円曲線 E と E 上の N 等分点の基底 P, Q で $e_N(P,Q) = \exp(2\pi i/N)$ となるものの組に対応している. ここで, $e_N(P,Q)$ は Weil pairing である.

定義 2.3 (保型形式, カスプ形式). $\mathbb{H}$ から $\mathbb{C}$ への正則関数 f が次を満たすとき f を重さ k, レベル N の**保型形式**という.

1. $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ に対して $f(\gamma z) = (cz+d)^k f(z)$.

2. f はすべてのカスプで正則. つまり, 任意の $SL_2(\mathbb{Z})$ の元 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対して

$$f(\gamma z) = \sum_{n=0}^{\infty} a(n,\gamma) q^{\frac{n}{N}} \quad (q = e^{2\pi i z})$$

と展開される. このフーリエ展開を q 展開と呼ぶことにする. 条件の 2 において定数項が現れない場合, つまり $a(0,\gamma)=0$ が成り立つとき f を重さ k, レベル N の**カスプ形式**という.

以下のように, 重さ k, レベル N の保型形式全体のなす集合を $M_k(N)$ とし, 重さ k, レベル N のカスプ形式全体のなす集合を $S_k(N)$ とする.

$$M_k(N) := \{f : \mathbb{H} \to \mathbb{C} | f \text{ は重さ } k, \text{ レベル } N \text{ の保型形式 }\},$$
$$S_k(N) := \{f : \mathbb{H} \to \mathbb{C} | f \text{ は重さ } k, \text{ レベル } N \text{ のカスプ形式 }\}.$$

$M_k(N)$, $S_k(N)$ は $\mathbb{C}$ 上の有限次元ベクトル空間となることが知られている [4].

次に, ある合同部分群 Γ' の保型形式とある合同部分群 Γ'' の保型形式との関係について述べる.

定義 2.4 (ディリクレ指標). $\mathbb{Z}$ から $\mathbb{C}^*$ への関数 χ が次の 3 条件

1. $\forall n \in \mathbb{Z}$ に対し $\chi(n+m)=\chi(n)$,
2. $\forall k, n \in \mathbb{Z}$ に対し $\chi(kn)=\chi(k)\chi(n)$,
3. $\chi(n) \neq 0 \leftrightarrow (n,m)=1$.

を満たすとき, χ を m を法とする**ディリクレ指標**という.

$f(z)=\sum a_n q^n \in M_k(\Gamma)$ とする. このとき, ディリクレ指標 χ に対して $f_\chi(z)=\sum a_n \chi(n) q^n$ を f の指標 χ による**ツイスト**という. このとき $f_\chi(z)$ は Γ より小さいある部分群において保型形式になることが知られている [4, p.137].

χ を N を法とするディリクレ指標とし,

$$f(z)|[\gamma]_k := (cz+d)^{-k} f(\gamma z), \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

と定義する.

任意の $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ に対して $f(z)|[\gamma]_k = (cz+d)^{-k} f(\gamma z)$ となる $f(z)$ から構成される $M_k(\Gamma_1)$ の部分空間 $M_k(N,\chi)$ を次のように定める. 同様に $S_k(N,\chi)$ を次の共通集合として定める.

$$M_k(N,\chi) := \{f \in M_k(\Gamma_1(N)) | \forall \gamma \in \Gamma_0(N) \text{ に対して } f[\gamma]_k = \chi(d) f\},$$
$$S_k(N,\chi) := M_k(N,\chi) \cap S_k(\Gamma_1(N))$$

と定義する.

次に Hecke 作用素 について解説する. Hecke 作用素 を考える理由は, Hecke 作用素に対し保型形式 f が同時固有形式となるときに, f に対応する L 関数がオイラー積表示を持つという性質を持っているためである.

Hecke 作用素 の定義の準備をする. 以下 G を群とする.

定義 2.5 (通約可能). Γ_1, Γ_2 を G の部分群とする. $[\Gamma_1 : \Gamma_1 \cap \Gamma_2] < \infty, [\Gamma_2 : \Gamma_1 \cap \Gamma_2] < \infty$ となるとき, Γ_1 と Γ_2 は通約可能という.

例 2.6. $\Gamma = SL_2(\mathbb{Z})$ とする. Γ' を Γ のレベル N の合同部分群とし, $\alpha \in G = GL_2^+$ であるとする. このとき, Γ' と $\alpha^{-}\Gamma'\alpha$ は通約可能である. なぜならば, ある整数 D で, $\Gamma' \cap \alpha^{-1}\Gamma'\alpha \supset \Gamma(ND)$ かつ $\Gamma' \cap \alpha\Gamma'\alpha^{-1}$ となり $\Gamma'' = \Gamma' \cap \alpha^{-1}\Gamma'\alpha$ とすれば, $\Gamma'' \supset \Gamma(N)$ かつ $\alpha\Gamma''\alpha^{-1} \supset \Gamma(ND)$ となるからである.

定義 2.7 (両側剰余類). $\Gamma_1, \Gamma_2 \subset G$ であり $\alpha \in G$ とする. 両側剰余類 $\Gamma_1\alpha\Gamma_2$ とは, $\gamma_1\alpha\gamma_2 \quad (\gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2)$ の形の G の元すべてのなす集合である.

上で $\Gamma_1\alpha\Gamma_2$ は右剰余類 $\Gamma_1\alpha$ を含み, 一般に $\Gamma_1\alpha\gamma_2$ という形の右剰余類の和集合であることを注意しておく. Γ' を群 G の部分群とし, $\alpha \in G$ を Γ' と $\alpha^{-1}\Gamma'\alpha$ が通約可能である任意の元とする. Γ'' を $\Gamma' \cap \alpha^{-1}\Gamma'\alpha$ とし, $[\Gamma' : \Gamma''] = d$ とする. このとき, $\Gamma' = \bigcup_{j=1}^{d} \Gamma''\gamma_j'$ と書けば

$$\Gamma'\alpha\Gamma' = \bigcup_{j=1}^{d} \Gamma'\alpha\gamma_j'$$

は d 個の右剰余類の交わりのない和集合となる. また, $\Gamma'\alpha\Gamma' = \bigcup_{j=1}^{d} \Gamma'\alpha\gamma_j'$ が d 個の右剰余類の交わりのない和集合ならば $\Gamma' = \bigcup_{j=1}^{d} \Gamma''\gamma_j'$ となる.

ここで, S^+ を $\mathbb{Z}$ の 0 でない部分群, つまりある正整数 M に対して $S^+ = M\mathbb{Z}$ とし, S^* を $(\mathbb{Z}/N\mathbb{Z})^*$ の部分群とする. ここで注意として N を法として $(\mathbb{Z}/N\mathbb{Z})^*$ に属する整数も S^* の元とする. n を正の整数とするとき

$$\Delta^n(N, S^*, S^+) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \middle| N|c, a \in S^*, b \in S^+, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}$$

と定義する.

例 2.8.

$$\Gamma_1(N) := \Delta^1(N, 1, \mathbb{Z}), \Gamma_0(N) := \Delta^1(N, (\mathbb{Z}/N\mathbb{Z})^*, \mathbb{Z}), \Gamma(N) := \Delta^1(N, 1, N\mathbb{Z}).$$

が例として挙げられる.

定義 2.9. Γ' を $\Gamma = SL_2(\mathbb{Z})$ の部分群, α を $GL_2''^+(\mathbb{Q})$ の元とする. $\Gamma'' = \Gamma' \cap \alpha^{-1}\Gamma'\alpha$ とし $[\Gamma' : \Gamma''] = d, \Gamma' = \bigcup_{j=1}^{d} \Gamma''\gamma_j'$ であるとする. $f(z)$ を $\gamma \in \Gamma'$ に対する $[\gamma]_k$ で不変な $\mathbb{H}$ 上の関数とするとき

$$f(z)|[\Gamma'\alpha\Gamma']_k := \sum_{j=1}^{d} f(z)|[\alpha\gamma_j']_k$$

と定義する.

$f(z)|[\Gamma'\alpha\Gamma']_k$ は代表元の選び方によらないで定まる．また，$f \in M_k(\Gamma')$ ならば $f|[\Gamma'\alpha\Gamma']_k \in M_k(\Gamma')$ である．ここまでの準備で正の整数 n に対して Hecke 作用素 T_n を定義する．

定義 2.10 (**Hecke 作用素**)**.** $\Gamma' = \Delta^1(N, S^*, S^+)$, n を正の整数とする．$f \in M_k(\Gamma')$ としたとき, 次の様に定義する．

$$T_n f := n^{\frac{k}{2}-1} \sum f|[\Gamma'\alpha\Gamma'].$$

和は $\Delta^n(N, S^*, S^+)$ に含まれる Γ' に関する両側剰余類をわたる．このとき, $T_n f \in M_k(\Gamma')$ となる．

g.c.d.$(m, n) = 1$ ならば $T_{mn} = T_m T_n$ であり, 特に T_m と T_n は可換である．

命題 2.11. 保型形式 f に対して Hecke 作用素 T_p は次の様に作用する．

$$T_p(f)(x) = \begin{cases} \dfrac{1}{p}\displaystyle\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + p^{k-1} f(pz) & \text{if } p \nmid N \\ \dfrac{1}{p}\displaystyle\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) & \text{if } p \mid N \end{cases}$$

次に newform と呼ばれる保型形式を定義する．newform とは大雑把に述べれば N を割るようなレベルからきた保型形式ではない保型形式のことである．

定義 2.12 (**ピーターソン内積**)**.** f_1, f_2 を重さ k, レベル N の保型形式とし, すくなくとも一方はカスプ形式とする．このとき, 内積 $\langle , \rangle$ を次のように定める．ここで少なくとも一方はカスプ形式であるとしたのは積分の収束性を保証するためである．

$$\langle f_1, f_2 \rangle = \frac{\mu(SL_2(\mathbb{Z}))}{\mu(\Gamma_0(N))} \int_{\mathbb{H}/\Gamma_0(N)} f_1(z)\overline{f_2(z)} y^k \frac{dxdy}{y^2}.$$

ここで, $\mu(\Gamma) = \displaystyle\int_{\mathbb{H}/\Gamma} \frac{dxdy}{y^2}$ とする．この $\langle\ ,\ \rangle$ をピータソン内積という．

newform を以下のように定義する．

定義 2.13 (**newform**)**.** $S_k^1(N)$ を $\displaystyle\bigcup_M \bigcup_l \{f(lz) | f(z) \in S_k(N)\}$ で生成される $S_k(N)$ の部分空間として定義する．ここで, M は N の真の約数, l は N/M の約数を走る．S_k^{new} を $\langle , \rangle$ に関する $S_k^1(N)$ の直交補空間として定義し, newform の空間という．

先ほど述べたように, レベル N のあるカスプ形式 f が newform であることがわかれば f はレベル N を割るようなレベルからきたカスプ形式ではないことがわかる．

2.3 半整数重さの保型形式

この節では半整数重さの保型形式について触れる．半整数重さの保型形式は特にテータ関数を扱うものであることに注意しておく．半整数重さに今まで通りの定義を適応すると $(cz+d)^{\frac{k}{2}}$ が等式の中にでできてしまい, $(cz+d)^{\frac{k}{2}}$ には分枝が 2 通りあるので, 2 次指標を使った新しい定義を与えなくてはならない.

$T=\{\pm 1,\pm i\}$, $GL_2^+(\mathbb{Q})=\{g\in GL_2(\mathbb{Q})|\det g>0\}$ とする．また G を次の様におく.

$$G=\left\{(\alpha,\phi(z))\;\middle|\;\begin{array}{c}\alpha=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in GL_2^+(\mathbb{Q}),\phi:\mathbb{H}\\ \text{上の正則関数である } t\in T^2 \text{ があって}\\ \phi(z)^2=t(\det\alpha)^{-\frac{1}{2}}(cz+d)\end{array}\right\}.$$

さらに G に次のように演算を入れると群となる.

$$(\alpha,\phi)\cdot(\beta,\psi):=(\alpha\beta,\phi(\beta z)\psi(z)).$$

$\xi=(\alpha,\phi(z))\in G$ と任意の整数 k に対し, $\mathbb{H}$ の関数 f への作用素 $[\xi]_{k/2}$ を次で定義する.

$$f(z)|[\xi]_{\frac{k}{2}}:=f(\alpha z)\phi(z)^{-k}.$$

$\Gamma':\Gamma_0(4)$ の部分群. $\gamma\in\Gamma'$ に対して $j(\gamma,z):=\theta(\gamma z)/\theta(\gamma)$ と定める.

$$\widetilde{\Gamma'}:=\{(\gamma,j(\gamma,z))|\gamma\in\Gamma'\}$$

と定める．このとき半整数重さの保型形式を次のように定義する.

定義 2.14 (半整数重さの保型形式). f を $\mathbb{H}$ から $\mathbb{C}$ への正則関数とする．f が重さ $\frac{k}{2}$ の保型形式であるとは

1. $\tilde{\gamma}\in\widetilde{\Gamma'}$ に対して $f(z)[\tilde{\gamma}]_{\frac{k}{2}}=f(z)$.
2. f はすべてのカスプで正則.

となるときである.

半整数重さの保型形式にも Hecke 作用素が定義されるが Hecke 作用素の指数が完全平方数 n^2 のときのみ非自明となる．よって, 半整数重さの場合の T_{n^2}, g.c.d.$(n,N)=1$ の生成元は N を割らない素数 p による T_{p^2} となる.

半整数重さの Hecke 作用素が完全平方数のときのみ非自明となることを示す.

$$G^1=\{(\alpha,\phi(z))\in G|\alpha\in\Gamma\},$$
$$\tilde{\Gamma}_0(4)=\left\{(\alpha,j(\alpha,z))\middle|\alpha=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(4),j(\alpha,z)=\left(\frac{c}{d}\right)\epsilon_d^{-1}(cz+d)^{\frac{1}{2}}\right\}.$$

また,

$$\xi_n = \left(\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, n^{\frac{1}{4}} \right)$$

とし,

$$f|[\tilde{\Gamma}_1(N)\tilde{\xi}_n\tilde{\Gamma}_1(N)]_{k/2} := \sum_j f|[\tilde{\xi}_n\tilde{\gamma}_j]_{k/2}$$

と定義する. ここで和は, 両側剰余類 $\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)$ に含まれる $\tilde{\Gamma}_1(N)$ に関する任意の相異なる右剰余類を走る.

命題 2.15. n を N と互いに素な完全平方数ではない正の整数とする. このとき,

$$f|[\tilde{\Gamma}_1(N)\tilde{\xi}_n\tilde{\Gamma}_1(N)]_{k/2} = 0$$

である.

証明. 与えられた $\alpha \in GL_2^+(\mathbb{Q})$ と $\xi = (\alpha, \phi) \in G$ に対し, $\Gamma' := \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$ から $T = \{\pm 1, \pm i\}$ への写像を次の様に構成する. ここで, $\gamma, \gamma_1 \in \Gamma_1(N)$ で $\gamma = \alpha^{-1}\gamma_1\alpha$ となる γ, γ_1 が与えられたとき, $\tilde{\gamma}, \xi^{-1}\tilde{\gamma}_1\xi \in G^1$ は共に Γ への同じ射影 γ を持つことに注意する. したがって,

$$\xi^{-1}\tilde{\gamma}_1\xi = \tilde{\gamma}(I_2, t).$$

と書ける.

固定された α, ξ に対して, γ に数 t を対応させる写像を考える. この写像 $t(\gamma)$ は α にのみ依存する Γ' から T への準同型となり, $\xi = (\alpha, \phi)$ の ϕ の選び方には依らず, $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$ の場合は

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma' = \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$$

に対して

$$t(\gamma) = \left(\frac{d}{n}\right)$$

となることがわかる. この写像の核を $K(\subset \Gamma')$ とおく.

$$\tilde{\Gamma}'' := \xi_n^{-1}\tilde{\Gamma}_1(N)\xi_n \cap \tilde{\Gamma}_1(N)$$

と定義すれば

$$\tilde{K} = \tilde{\Gamma}''$$

となる. これを示す. $\gamma, \gamma_1 \in \Gamma_1(N)$ で $\tilde{\gamma}\xi_n^{-1}\tilde{\gamma}_1\xi_n$ であると仮定する. 射影 $P : G \to GL_2^+(\mathbb{Q})$ を適応すると

$$\gamma = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}^{-1} \gamma_1\alpha$$

であり,

$$\gamma \in \Gamma' = \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$$

となる. $\xi^{-1}\tilde{\gamma_1}\xi_n = \tilde{\gamma} = \tilde{\gamma}(I_2, t)$ なので $\gamma \in K$ となる.

逆は, $\gamma \in K \subset \Gamma'$ ならば $\gamma = \alpha^{-1}\gamma_1\alpha$ で $\xi_n^{-1}\tilde{\gamma_1}\alpha = \tilde{\gamma}(I_2, t), t = t(\gamma) = 1$ となるので, $\tilde{\gamma} \in \tilde{\Gamma}''$ となる.

一般に $\tilde{\Gamma}'' = \tilde{K}$ は $\tilde{\Gamma}'$ に含まれる. つまり, $\xi_n^{-1}\tilde{\Gamma}_1\xi_n \cap \tilde{\Gamma}_1(N)$ は $\Gamma' = \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$ のリフトの部分群である. $\tilde{\Gamma}''$ と $\tilde{\Gamma}'$ が一致するには, 写像 t が自明となることが必要十分である. 今 $t(\gamma) = \left(\frac{d}{n}\right)$ なので, 写像 t が自明であるためには n が完全平方数であることが必要十分である.

n が完全平方数でないとき, $\tilde{\Gamma}''$ は $\tilde{\Gamma}'$ の指数 2 の部分群である. $\tilde{\Gamma}' = \tilde{\Gamma}'' \cup \tilde{\Gamma}''\tilde{\tau}$ を右剰余類分解とすれば, $\tau = \alpha^{-1}\tau_1\alpha$ で $\tilde{\tau} = \xi_n^{-1}\tilde{\tau_1}\xi_n \cdot (I_2, -1)$ となる. $\Gamma_1(N)$ の Γ' に関する右剰余類分解を $\Gamma_1(N) = \bigcup_j \Gamma'\gamma_j$ とすると

$$\tilde{\Gamma}_1(N) = \bigcup_j \tilde{\Gamma}''\tilde{\gamma}_j \cup \bigcup_j \tilde{\Gamma}''\tilde{\tau}\tilde{\gamma}_j$$

が $\tilde{\Gamma}_1(N)$ の $\tilde{\Gamma}''$ に関する右剰余類分解である. このとき,

$$f|[\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)]_{k/2} = \sum_j f|[\xi_n\tilde{\gamma}_j]_{k/2} + \sum_j f|[\xi\tilde{\tau}\tilde{\gamma}_j]_{k/2}$$

が成り立つ. しかし, f は $\tilde{\tau_1} \in \tilde{\Gamma}_1(N)$ に対する $[\tilde{\tau_1}]_{k/2}$ で不変であるので,

$$\begin{aligned} f|[\xi_n\tilde{\tau}\tilde{\gamma}_j]_{k/2} &= f|[\xi_n\tilde{\tau}\xi_n^{-1}\xi_n\tilde{\gamma}_j]_{k/2} \\ &= f|[\tilde{\tau_1}(I_2, -1)\xi_n\tilde{\gamma}_j]_{k/2} \\ &= f|[(I_2, -1)\xi_n\tilde{\gamma}_j]_{k/2} \end{aligned}$$

となる. 定義より $[(I_2, -1)]_{k/2} = (-1)^k = -1$ となるので

$$f|[\xi_n\tilde{\gamma}_j]_{k/2} + f|[\xi_n\tilde{\tau}\tilde{\gamma}_j]_{k/2} = f|[\xi_n\tilde{\gamma}_j]_{k/2} - f|[\xi_n\tilde{\gamma}_j]_{k/2} = 0$$

である. □

命題 2.15 により, 半整数重さの Hecke 作用素 は完全平方数 n^2 のときのみ非自明となる.

命題 2.16. $g(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{k/2}(N, \chi)$ に対して Hecke 作用素 T_{p^2} に対して

$$T_{p^2}(g)(z) = \sum_{n=0}^{\infty} b(n)q^n$$

が成り立つ. $\lambda = \dfrac{k-1}{2}$ とすれば $b(n)$ は

$$b(n) = a(p^2n) + \chi(p)\left(\frac{-1}{p}\right)^{\lambda}\left(\frac{n}{p}\right)p^{\lambda-1}a(n) + \chi(p^2)p^{2\lambda-1}a(n/p^2).$$

ただし, $a(n/p^2)$ は $p^2 \nmid n$ のときは 0.

志村対応 [13] を解説する. k を 3 以上の奇数とする. $\lambda = \dfrac{k-1}{2}$, N は 4 で割り切れ, χ は法 N のディリクレ指標とする. $f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_{k/2}(\tilde{\Gamma}_0(N), \chi)$ を任意の素数 p に対する T_{p^2} の同時固有形式で固有値が λ_p であるものとする. 関数

$$\mathrm{SH}(f)(z) = \sum_{n=1}^{\infty} b_n q^n$$

を次の恒等式で定める.

$$\sum_{n=1}^{\infty} b_n n^{-s} = \prod_{p} \frac{1}{1 - \lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}}.$$

このとき, χ^2 のコンダクターで割り切れるある正整数 N' に対して $\mathrm{SH}(f)(z) \in M_{k-1}(N', \chi^2)$ となる. さらに, $k \geq 5$ のときは, $\mathrm{SH}(f)$ はカスプ形式であることが志村 [13] により示された. また, Niwa [9] により N' は $N/2$ とすればよいことが示された.

志村対応の仮定を満たす 1 次独立なカスプ形式 $f_i \in S_{k/2}(\tilde{\Gamma}_0(N), \chi)$ からなる集合を一つ固定したとする. すると, 志村対応を f_i で張られる $S_{k/2}(\tilde{\Gamma}_0(N), \chi)$ の部分空間に (線型性により) 拡張できる. ここで, f_i の志村対応による像 g_i は常に正規化された固有形式を意味することに注意する.

また, $\mathrm{SH}(f_i) = g_i$ を満たす固有形式 f_i を基底に持つ保型形式の空間を考えるときは $\mathrm{SH}(\sum a_i f_i) = \sum a_i g_i$ と定義する. このときは, 正規化された固有形式とは限らない.

一般に異なる同時固有形式 $f \in S_{k/2}(\tilde{\Gamma}_0(N), \chi)$ が同じ $g \in M_{k-1}(\Gamma_0(N'), \chi^2)$ に志村対応で写ることがある. 例えば, $\chi \neq \chi'$ で $\chi^2 = \chi'^2$ となる指標 χ' に対して, 志村対応で g に対応する $f' \in S_{k/2}(\tilde{\Gamma}_0(N), \chi')$ が存在する可能性がある. $N = 4$ の場合は Kohnen [5] により研究がなされている.

3　合同数問題

3.1　合同数と楕円曲線

この節では合同数と楕円曲線との関係について述べる.

命題 3.1. n を平方因子を持たない自然数とする. X, Y, Z, x を正の整数とし $X < Y < Z$ となっているものとする. 面積 n の斜辺 Z, その他の 2 辺が X, Y の直角三角形全体の集合と $x, x+n, x-n$ がそれぞれ有理数の平方となる x の全体の集合とに次のような 1 : 1 対応が存在する.

$$\begin{aligned} X, Y, Z &\longrightarrow x = (Z/2)^2, \\ x &\longrightarrow X = \sqrt{x+n} - \sqrt{x-n}, \\ & \quad\ Y = \sqrt{x+n} + \sqrt{x-n}, \\ & \quad\ Z = 2\sqrt{x}. \end{aligned}$$

特に n が合同数であることと $x, x+n, x-n$ が有理数の平方となる x が存在することとは同値である.

証明. この対応がうまく定まっていることを確認する. X, Y, Z を面積が n となる直角三角形の 3 辺と仮定する. つまり以下の 2 式が成り立っているとする.

$$X^2 + Y^2 = Z^2, \tag{3.2}$$

$$\frac{XY}{2} = n. \tag{3.3}$$

(3.2) に (3.3) の 4 倍を足す (引く) ことにより

$$(X \pm Y)^2 = Z^2 \pm 4n.$$

さらに両辺を 4 で割ると

$$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n.$$

よって $x = (Z/2)^2$ は $x \pm n$ が有理数の平方になることが示された. 逆に $x, x+n, x-n$ が有理数の平方となる x が与えられたとき, 命題中の対応で与えられる正の有理数 X, Y, Z は (3.2), (3.3) を満たすことは計算より明らかである. 全射性は上の議論より良い. 単射性を確認する.

$x = (Z/2)^2$ を 1 つ固定すると (Z を 1 つ固定すると), C_1, C_2 を定数として下の 2 つの式を満たす正の有理数 $X < Y$ の組 (X, Y) が唯一定まることをいえば良い.

$$\begin{aligned} X + Y &= C_1, \\ XY &= C_2. \end{aligned}$$

しかし解と係数との関係よりこのような (X, Y) は一意的に定まる. □

上の命題の証明中に現れた次の 2 式

$$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n$$

を掛け合わせると

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$$

を得る. このことは, 方程式 $u^2 = v^4 - n^2$ が有理数解 $u = (X^2 - Y^2)/4, v = Z/2$ を持つことを示している. 両辺に v^2 を掛けると $(uv)^2 = v^6 - n^2v^2$ となる. $x = v^2 = (Z/2)^2$, $y = uv = (X^2 - Y^2)Z/8$ とおくと, 有理数の組 (x, y) で

$$y^2 = x^3 - n^2x$$

を満たすものが得られる. $y^2 = x^3 - n^2x$ は楕円曲線となっている. この楕円曲線を以後 E_n と書く.

よって, 平方因子を持たない自然数 n を面積に持つような有理数辺 X, Y, Z を持つ直角三角形が与えられたとき, 楕円曲線 $E_n : y^2 = x^3 - n^2x$ 上の有理点 (x, y) が得られる. しかし, 楕円曲線 $E_n : y^2 = x^3 - n^2x$ の任意の有理点が面積 n の有理数辺を持つ直角三角形に対応しているわけではなく次の制限がつく.

命題 3.4. (x, y) を楕円曲線 $E_n : y^2 = x^3 - n^2x$ の有理点とする. x が次の 3 条件を満たすと仮定する.

1. x は有理数の平方である.
2. x の分母は偶数である.
3. x の分子と n は互いに素である.

このとき, 面積 n の有理数の 3 辺 X, Y, X を持つ直角三角形が存在して以下の対応により x と対応する.

$$\begin{aligned} X, Y, Z &\longrightarrow x = (Z/2)^2, \\ x &\longrightarrow X = \sqrt{x+n} - \sqrt{x-n}, \\ & \quad\ Y = \sqrt{x+n} + \sqrt{x-n}, \\ & \quad\ Z = 2\sqrt{x}. \end{aligned}$$

証明. (x, y) を上の 3 つの仮定を満たす楕円曲線 E_n の有理点とする. $u, v \in \mathbb{Q}$ を $u = \sqrt{x}, v = y/u$ とおく. よって, $v^2 = y^2/x = x^2 - n^2$ となり $v^2 + n^2 = x^2$ となる. t を u の分母とする. 仮定より u の分母 t は偶数である. n は自然数なので $v^2 + n^2 = x^2, u^2 = x$ より v^2, x^2 の分母は等しく t^4 であることがわかる. したがって, t^2v, t^2n, t^2x は互いに素なピタゴラスの 3 つ組であり t^2n は偶数である. ここで以下の補題を用いる.

補題 3.5. a と b を $a > b$ となる互いに素な正整数とし, どちらか一方は偶数とする. このとき,

$$X = a^2 - b^2, \quad Y = 2ab, \quad Z = a^2 + b^2.$$

は互いに素なピタゴラスの 3 つ組となる. また, 互いに素なピタゴラスの 3 つ組はこのようにして得られる.

補題 3.5 より正整数 a, b で $t^2v = a^2 - b^2, t^2n = 2ab, t^2x = a^2 + b^2$ となるものが存在する. このとき $n = 2ab/t^2$ を面積とし 3 辺が $2a/t, 2b/t, 2u$ である直角三角形が求めたいものとなっている. □

$E_n(\mathbb{F}_q)$ の $q \equiv 3 \mod 4$ での位数を与える. $q \equiv 1 \mod 4$ での位数に関しては後で述べる.

命題 3.6. $q = p^f, p \nmid 2n$ とする. $q \equiv 3 \mod 4$ と仮定する. このとき,

$$\#E_n(\mathbb{F}_q) = q + 1.$$

証明. 位数が 2 以下の点は次の 4 つである. $O, (0,0), (n,0), (-n,0)$. 今, $x \neq 0, n, -n$ となるすべての対 (x, y) を数える. これらの $q - 3$ 個の x を対 $\{x, -x\}$ にして並べる. $f(x) = x^3 - n^2x$ は奇関数であり $q \equiv 3 \mod 4$ より -1 は $\mathbb{F}_q$ で平方元でない. したがって, $f(x)$ か $f(-x) = -f(x)$ のどちらか一方のみが $\mathbb{F}_q$ で平方元となる. $(x, \pm\sqrt{f(x)})$ または $(-x, \pm\sqrt{f(-x)})$ のうちの 2 点が $\mathbb{F}_q$ 有理点として得られる. 以上より $(q-2)/2$ 個の対は $q - 3$ 個の点を与える. 位数 2 以下の点と合わせて $q + 1$ 個の $\mathbb{F}_q$ 有理点を得た. □

今, 私たちが考えていた楕円曲線 E_n の torsion part は n に依らずに以下の様に決定できる.

命題 3.7. $\#E_n(\mathbb{Q})_{\mathrm{tors}} = 4$.

証明. $E_n(\mathbb{Q})_{\mathrm{tors}}$ から $E_n(\mathbb{F}_p)$ への準同型写像で多くの p に対して単射であるものを構成したい. すると, そのような p に対して $E_n(\mathbb{Q})_{\mathrm{tors}}$ の位数は $E_n(\mathbb{F}_p)$ を割り切ることがわかる. しかし, 4 より大きい整数でそのようなすべての数が $\#E_n(\mathbb{F}_p)$ を割り切るものはないことが上の命題からわかるからである.

目的の準同型写像を構成する. まず, $\mathbb{P}^2_{\mathbb{Q}}$ から $\mathbb{P}^2_{\mathbb{F}_p}$ への写像を構成する. これからは $\mathbb{P}^2_{\mathbb{Q}}$ の元 (x, y, z) を x, y, z は整数で共通因子を持たないものをとる. $\pm$ の差を除けば各同値類にそのような x, y, z の 3 つ組はただ 1 つ存在する. 任意の素数 p に対して, $P = (x, y, z) \in \mathbb{P}^2_{\mathbb{Q}}$ の像 $\bar{P}$ を, 点 $\bar{P} = (\bar{x}, \bar{y}, \bar{z}) \in \mathbb{P}^2_{\mathbb{F}_p}$ と定義する. p は 3 つの整数 x, y, z を同時に割り切ることはないから $\bar{P}$ は $(\bar{0}, \bar{0}, \bar{0})$ にはならないことに注意しておく. また, 3 つ組 (x, y, z) を p と素な整数を掛けたものと取り換えても $\bar{P}$ には影響しないことを注意しておく.

$P = (x, y, z)$ が $E_n(\mathbb{Q})$ の元ならば $\bar{P}$ は $E_n(\mathbb{F}_p)$ の元であることは明らかである. また, 楕円曲線の加法公式は和を求めて p で還元することと, 還元してから和を取る

ことは同じなので P_1+P_2 のこの写像での像は $\bar{P_1}+\bar{P_2}$ である. つまり, この写像は $E_n(\mathbb{Q})$ から $E_n(\mathbb{F}_p)$ への準同型写像である. この写像が単射とならない場合を考える. つまり $\mathbb{P}^2_{\mathbb{Q}}$ の 2 点 $P_1=(x_1,y_1,z_1), P_2=(x_2,y_2,z_2)$ が $\mathbb{P}^2_{\mathbb{F}_p}$ で同一の像 $\bar{P_1}=\bar{P_2}$ を持つ場合を決定する. それが次の補題である.

補題 3.8. $\bar{P_1}=\bar{P_2}$ であることと p が $y_1z_2-y_2z_1, x_2z_1-x_1z_2, x_1y_2-x_2y_1$ を割り切ることが必要十分である.

証明. この補題は $\bar{P_1}=\bar{P_2}$ であるためには, P_1 と P_2 の $\mathbb{R}^3$ のベクトルと考えたときの外積が p で割り切れることとが同値である主張である. まず p が外積を割り切ると仮定する. 次の 2 つの場合を考える.
(i) p が x_1 を割り切る場合: このとき , p は x_2z_1, x_2y_1 を割り切り x_1, y_1, z_2 は同時に p で割り切れることはないので x_2 が p で割り切れることがわかる. ここで $p\nmid y_1$ とし $p|y_1z_2-y_2z_1$ に注意すれば,

$$\bar{P_2}=(\bar{x}_2,\bar{y}_2,\bar{z}_2)=(0,\bar{y}_1\bar{y}_2,\bar{y}_1\bar{z}_2)=(0,\bar{y}_1\bar{y}_2,\bar{y}_2\bar{z}_1)=(0,\bar{y}_1,\bar{z}_1)=\bar{P_1}$$

となる. $p\nmid z_1$ としても同様である.
(ii) p が x_1 を割り切らない場合: このとき,

$$\bar{P_2}=(\bar{x}_2,\bar{y}_2,\bar{z}_2)=(\bar{x}_1\bar{x}_2,\bar{x}_1\bar{y}_2,\bar{x}_1\bar{z}_2)=(\bar{x}_1\bar{x}_2,\bar{x}_2\bar{y}_1,\bar{x}_2\bar{z}_1)=(\bar{x}_1,\bar{y}_1,\bar{z}_1)=\bar{P_1}$$

となる.

$\bar{P_1}=\bar{P_2}$ と仮定する. 一般性を失うことなく $p\nmid x_1$ とでき, このとき $p\nmid x_2$ であり,

$$(\bar{x}_1\bar{x}_2,\bar{x}_1\bar{y}_2,\bar{x}_1\bar{z}_2)=(\bar{x}_2,\bar{y}_2,\bar{z}_2)=\bar{P_2}=\bar{P_1}=(\bar{x}_1,\bar{y}_1,\bar{z}_1)=(\bar{x}_2\bar{x}_1,\bar{x}_2\bar{y}_1,\bar{x}_2\bar{z}_1)$$

となる. $\bar{P_1},\bar{P_2}$ は第 1 成分が等しいので第 2 成分と第 3 成分が等しいときに等しい点となる. つまり p が $x_1y_2-x_2y_1, x_1z_2-x_2z_1$ を割り切るときに限り等しくなる. よって最後に確認しなくてはならないのが p が $y_1z_2-y_2z_1$ を割り切ることである. y_1 と y_2 が p で割り切れるときは明らかである. そうでないときは上と同様の議論より従う. つまり, $p\nmid y_1$ とすれば $\bar{P_1}=\bar{P_2}$ より $p\nmid y_2$ がわかり

$$(\bar{y}_1\bar{x}_2,\bar{y}_1\bar{y}_2,\bar{y}_1\bar{z}_2)=(\bar{x}_2,\bar{y}_2,\bar{z}_2)=\bar{P_2}=\bar{P_1}=(\bar{x}_1,\bar{y}_1,\bar{z}_1)=(\bar{y}_2\bar{x}_1,\bar{y}_2\bar{y}_1,\bar{y}_2\bar{z}_1)$$

となるので p が $y_1z_2-y_2z_1$ を割り切ることがわかる. 他の場合も同様なので省略する. □

以上で補題 (3.8) の証明が完成した. 命題 (3.7) の証明に戻る. 命題が偽であるとする. つまり, $E_n(\mathbb{Q})$ は位数が 2 以上の有限位数の点を含むとする. このとき $E_n(\mathbb{Q})$ は奇数位数の元を含むか, または位数 4 の約数の点のなす群が 8 個または 16 個の元を含む. どの場合にしても $E_n(\mathbb{Q})_{\mathrm{tors}}$ の位数 m が奇数か 8 となる部分群 $S=P_1,P_2,\ldots,P_m\subset E_n(\mathbb{Q})_{\mathrm{tors}}$ が存在する. 点 $P_i(i=1,\ldots,m)$ を $P_i(x_i,y_i,z_i)$ と書き表すこととする. 2 点 P_i,P_j に対して, 外積 $(y_iz_j-y_jz_i, x_jz_i-x_iz_j, x_iy_j-x_jy_i)\in\mathbb{R}^3$

を考える. P_i, P_j は射影平面内の相異なる点なので, スカラー倍ではない. よって, 外積は 0 ではない. n_{ij} を外積の各座標の最大公約数とする. 補題 (3.8) により P_i と P_j が $E_n(\mathbb{F}_p)$ において同じ像 $\bar{P}_i = \bar{P}_j$ を持つことと p が n_{ij} を割ることとは同値である. したがって p がすべての n_{ij} より大きいよい還元をもつ素数であればすべての像は異なることがわかる. つまり p を法とする還元写像は S から $E_n(\mathbb{F}_p)$ への単射となることがわかる. しかし, S の像は位数 m の部分群なので有限個を除く p が $\#E_n(\mathbb{F}_p)$ を割り切らないといけないことを意味している. このとき有限個を除く 4 を法として 3 と合同な素数 p に対して, 命題 (3.6) より $p \equiv -1 \mod m$ とならねばならない. このとき, $m = 8$ ならば $8k+3$ の形の素数が有限個, m が奇数ならば $3 \nmid m$ の時は $4mk+3$ の形の素数は有限個, $3|m$ の時は $12k+7$ の形の素数が有限個であることを主張しているが, Dirichlet の算術級数定理より上で与えられた形の素数は無限個存在することがわかるので矛盾となる. □

命題 (3.7) の系として合同数問題に非常に有用な命題を述べる.

命題 3.9. n が合同数であることと $E_n(\mathbb{Q})$ の階数 r が 0 より大きいこととは同値である.

証明. n が合同数であると仮定する. 面積 n の有理数の 3 辺を持つ直角三角形から楕円曲線 E_n の有理点が与えられ, その x 座標は有理数の平方となっていることは以前にみた. 位数 2 の 3 個の非自明な点の x 座標は $0, \pm n$ なので位数が 2 以下でない点が存在しなくてはならないことがわかる. 命題 (3.7) よりそのような点の位数は無限であることがわかり階数 r は 1 以上であることがわかる.

$E_n(\mathbb{Q})$ の階数 r が 0 より大きいと仮定し, P は無限位数の点であるとする. 点 P の 2 倍点 $2P$ は 2 倍点の公式より x 座標は有理数の平方であり, その分母は偶数である. 命題 (3.4) を用いるためには x 座標の分子が n と互いに素であることをいわなくてはいけない. つまり, n の各素因数 p に対して, $p \neq 2$ のとき $\mathrm{ord}_p(x^2+n^2) \leq \mathrm{ord}_p(y)$, $p = 2$ のとき $\mathrm{ord}_2(x^2+n^2) \leq \mathrm{ord}_2(2y)$ を示さなくてはいけない. いま, $p \neq 2$ のとき $\mathrm{ord}_p(x^2+n^2) \leq \mathrm{ord}_p(y)$ の場合を示す.
(1) $\mathrm{ord}_p(x) < \mathrm{ord}_p(n)$ の場合: $\mathrm{ord}_p(n) = 1$ より $\mathrm{ord}_p(x) \leq 0$. ゆえに $\mathrm{ord}_p(x^2+n^2) = 2\mathrm{ord}_p(x)$. $y^2 = x^2 - n^2x$ であるから $\mathrm{ord}_p(x^3) = \mathrm{ord}_p(y^2)$. つまり $\mathrm{ord}_p(x) = 2\mathrm{ord}_p(y)/3 \leq 3 < 0$ となる. よって

$$\mathrm{ord}_p(x^2+n^2) = 4\mathrm{ord}_p(y)/3 \leq \mathrm{ord}_p(y)$$

となる.
(2) $\mathrm{ord}_p(x) > \mathrm{ord}_p(n)$ の場合: $\mathrm{ord}_p(n) = 1$ であるから $\mathrm{ord}_p(x) \geq 2$ かつ $\mathrm{ord}_p(x^2+n^2) = 2$. $y^2 = x(x-n)(x+n)$ より $\mathrm{ord}_p(y^2) = \mathrm{ord}_p(x) + 2\mathrm{ord}_p(n)$ となり,

$$\mathrm{ord}_p(y) \geq 2 = \mathrm{ord}_p(x^2+n^2)$$

となる.
(3) $\mathrm{ord}_p(x) = \mathrm{ord}_p(n)$ の場合: $\mathrm{ord}_p(x) = 1$ なので $y^2 = x(x-n)(x+n)$ を用いて

$2\mathrm{ord}_p(y) \geq 3$. $2\mathrm{ord}_p(y)$ は偶数であるから, $\mathrm{ord}_p(y) \geq 2$. ここで $\mathrm{ord}_p(x^2+n^2) = 2$ であることを示す. $\mathrm{ord}_p(y) \geq 2$ と $y^2 = x(x-n)(x+n)$ より $\mathrm{ord}_p(x+n)+\mathrm{ord}_p(x-n) \geq 3$ となる. つまり, $\mathrm{ord}_p(x+n) \geq 2$ または $\mathrm{ord}_p(x-n) \geq 2$ となる. $x^2+n^2 = (x \pm n)^2 \mp 2xn$ より $\mathrm{ord}_p(x \pm n) \geq 2$ と考えると, $\mathrm{ord}_p(x^2+n^2) = 2$ がわかる. 命題 (3.4) より本命題が従う. □

命題 3.10. 面積 n で有理数の 3 辺 $X < Y < Z$ を持つ直角三角形と, 点の組 $(x, \pm) \in 2E_n(\mathbb{Q}) - \{O\}$ の間に 1 : 1 対応があり, その対応は以下の通りである.

$$\begin{array}{rcl} (x, \pm y) & \longrightarrow & \sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}, \\ X, Y, Z & \longrightarrow & (Z^2/4, \pm(Y^2 - X^2)Z/8) \end{array}$$

命題 (3.1) を考慮すれば, 命題 (3.10) は次の命題の特徴付けからわかる結果である.

命題 3.11. E を楕円曲線 $y^2 = (x-e_1)(x-e_2)(x-e_3) \quad (e_1, e_2, e_3) \in \mathbb{Q}$ とする. このとき, $P = (x_0, y_0) \in E(\mathbb{Q}) - \{O\}$ とする. このとき, $P \in E(\mathbb{Q}) - \{O\}$ であることと $x_0 - e_1, x_0 - e_2, x_0 - e_3$ が有理数の平方であることとは同値である.

証明. まず一般性を失うことなく, $x_0 = 0$ と仮定してよいことに注意する. なぜならば, 変数変換 $x' = x - x_0$ をするとグラフをただ平行移動するだけなので, 楕円曲線 $E' : y^2 = (x-e_1')(x-e_2')(x-e_3') \quad (e_i' = e_i - x_0)$ の上の点 $P' = (0, y_0)$ が $2E'(\mathbb{Q}) - \{O\}$ の元となるには, P が $2E(\mathbb{Q})$ の元になっていることが必要十分条件だからである. よって一般性を失うことなく $x_0 = 0$ と仮定してよいことがわかる.

次に, ほぼ明らかだが $Q \in E(\mathbb{Q})$ で $2Q = P$ となるものが存在すれば, ちょうど 4 つの点 $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ が存在して, $2Q_i = P$ となることに注意する.

$2Q = P = (0, y_0)$ となるような点 $Q = (x, y)$ を選ぶ. そのような 1 点 Q の座標が有理数となるための条件を求めていく. 楕円曲線上の点 Q が $2Q = P$ を満たすためには楕円曲線の Q における接線が $-P = (0, -y_0)$ を通ることが必要十分である. 必要条件であることはよい. 十分条件についてみやると, 傾き m が有理数であるとすると, Q の x 座標は 3 次方程式 $(mx - y_0)^2 = (x-e_1)(x-e_2)(x-e_3)$ の 2 重根であり, $x = (m^2 + e_1 + e_2 + e_3)/2$ となり有理数である. このとき, Q の y 座標も有理数 $y = mx - y_0$ となる. 以上より, $-P$ から E への接線の傾きがどのようなとき有理数となりうるかを調べたい.

m を複素数とする. m が上で述べた $-P$ から E に接する直線の傾きであるには次の方程式が 2 重根を持つことが必要十分条件となる.

$$(mx - y_0)^2 = (x-e_1)(x-e_2)(x-e_3) = x^3 + ax^2 + bx + c.$$

ここで

$$\begin{aligned} a &= -e_1 - e_2 - e_3, \\ b &= e_1e_2 + e_1e_3 + e_2e_3, \\ c &= -e_1e_2e_3 = y_0^2. \end{aligned}$$

上の条件は次の条件に書き換えられる.

$$x^2 + (a - m^2)x + (b + 2my_0) = 0.$$

が重根を持つ. つまり判別式が 0,

$$(a - m^2)^2 - 4(b + 2my_0) = 0$$

と同値である. よって, 上の m に関する 4 次の方程式の根がいつ有理数なるかを決定すればよい.

m が有理数であることと $-e_i$ が有理数の平方となることが同値であることを示したい. 判別式の各係数を対称式で表したいので $f_i^2 = -e_i$ となる f_i を導入する. $e_i = 0$ でない限り f_i には 2 通りの選び方があるが $y_0 = f_1 f_2 f_3$ という条件を満たすように任意に選んでよい. すると 4 通りの選び方が存在する.

$$\begin{array}{ccc} f_1 & f_2 & f_3, \\ f_1 & -f_2 & -f_3, \\ -f_1 & -f_2 & f_3, \\ -f_1 & f_2 & -f_3. \end{array} \tag{3.12}$$

この内の 1 つを固定し議論を進める. 基本対称式を次の様におく.

$$\begin{aligned} s_1 &= f_1 + f_2 + f_3, \\ s_2 &= f_1 f_2 + f_2 f_3 + f_1 f_3, \\ s_3 &= f_1 f_2 f_3. \end{aligned}$$

すると

$$\begin{aligned} a &= f_1^2 + f_2^2 + f_3^2 = s_1^2 - 2s_2, \\ b &= f_1^2 f_2^2 + f_1^2 f_3^2 + f_2^2 f_3^3 = s_2^2 - 2s_1 s_3, \\ y_0 &= s_3. \end{aligned}$$

となる. よって判別式は

$$(m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1) = 0.$$

この方程式は $m - s_1$ で割り切れる. よって $m = s_1 = f_1 + f_2 + f_3$ は根となる. f_i の選び方は 4 通りあったので m の 4 次の方程式の根は

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3, \\ m_2 &= f_1 - f_2 - f_3, \\ m_3 &= -f_1 - f_2 + f_3, \\ m_4 &= -f_1 + f_2 - f_3. \end{aligned}$$

である． m_1, m_2, m_3, m_4 の値が有理数であるか否かを知りたい． f_i が有理数ならば m_1, m_2, m_3, m_4 は有理数である． m_1, m_2, m_3, m_4 が有理数であれば $f_1 = (m_1 + m_2)/2, f_2 = (m_1 + m_3)/2, f_3 = (m_1 + m_4)/2$ は有理数である．以上より Q の x, y 座標が有理数であることと f_i が有理数であることとが同値であることがわかり証明が完了した． □

3.2 楕円曲線 E_n の L 関数

ここでは楕円曲線 E_n の L 関数についてみる. この L 関数の $s=1$ での値から楕円曲線 E_n のランクの情報を得ることができる. まず, 合同ゼータ関数を定義する.

定義 3.13 (合同ゼータ関数). V を $\mathbb{F}_q$ $(q=p^l)$ 上定義されたアフィン多様体または射影多様体とする. $\mathbb{F}_q$ を含む任意の体 K に対して, $V(K)$ を V の K 有理点の全体のなす集合とし, $N_r=\#V(\mathbb{F}_q^r)$ とする. V の $\mathbb{F}_q$ 上の合同ゼータ関数を次の様に定義する.

$$Z(V/\mathbb{F}_q;T):=\exp\left(\sum_{r=1}^{\infty}N_r\frac{T^r}{r}\right).$$

V が特に $\mathbb{F}_q$ 上の楕円曲線のときについてみていきたい. $\mathbb{F}_q$ 上で定義された任意の楕円曲線 E の合同ゼータ関数は以下の形になることが知られている.

$$Z(E/\mathbb{F}_q;T)=\frac{1-2a_ET+qT^2}{(1-T)(1-qT)}. \tag{3.14}$$

ここで, $2a_E$ は楕円曲線 E にのみ依存する整数であり

$$2a_E=q+1-\#E(\mathbb{F}_q)$$

である. α を分子 $1-2a_ET+qT^2$ の根の逆数とする. すると, $1-2a_ET+qT^2=(1-\alpha T)(1-(q/\alpha)T)$ となる.

このとき, (3.17) と次の式が同値であることがわかる.

$$N_r=q^r+1-\alpha^r-(q/\alpha)^r. \tag{3.15}$$

楕円曲線 $E_n: y^2=x^3-n^2x$ の場合も (3.15) を満たすことがわかり, 次の命題の様になっている.

命題 3.16. $p\not|2n$ とする. このとき,

$$Z(E_n/\mathbb{F}_p;T)=\frac{1-2a_{E_n}T+pT^2}{(1-T)(1-pT)}=\frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}. \tag{3.17}$$

ここで, $a_{E_n}=\mathrm{Re}\ \alpha$ であり, α は $p\equiv 3 \mod 4$ のとき, $i\sqrt{p}$. $p\equiv 1 \mod 4$ のとき, $\mathbb{Z}[i]$ でのノルムが p の元であり, $2+2i$ を法として $\left(\frac{n}{p}\right)$ と合同となるものである.

$Z(E_n/\mathbb{F}_p;T)$ に $T=p^{-s}$ を代入して楕円曲線 E_n の L 関数を定義する.

定義 3.18. 楕円曲線 E_n の L 関数 $L(E_n,s)$ を次の様に定義する.

$$L(E_n,s):=\frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p;p^{-s})}. \tag{3.19}$$

$L(E_n, s)$ は $\mathrm{Re}\ s > 3/2$ で収束する. 定義の分子 $\zeta(s)\zeta(s-1)$ は, 分母の合同ゼータ関数の $p|2n$ のときの因子 $1/(1-p^{-s})(1-p^{1-s})$ を打ち消し, $p|2n$ のときは積は 1 となり意味をなさない. また, L 関数は

$$L(E_n, s) = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E_n} p^{-s} + p^{1-2s}} \tag{3.20}$$

と書けることもわかる. L 関数はリーマンゼータ関数同様, オイラー積表示を展開してやることによりディリクレ級数

$$L(E_n, s) = \sum_{m=1}^{\infty} \frac{b_{m,n}}{m^s} \tag{3.21}$$

の表示を持つ.

例 3.22.

$$\begin{aligned} L(E_1, s) = \frac{1}{1 + 3 \cdot 9^{-s}} \cdot \frac{1}{1 + 2 \cdot 5^{-s} + 5 \cdot 25^{-s}} \cdot \frac{1}{1 + 7 \cdot 49^{-s}} \cdot \\ \times \frac{1}{1 + 11 \cdot 121^{-s}} \cdot \frac{1}{1 - 6 \cdot 13^{-s} + 13 \cdot 169^{-s}} \cdots \\ = 1 - 2 \cdot 5^{-s} - 3 \cdot 9^{-s} + 6 \cdot 13^{-s} + \sum_{m \geq 17} \frac{b_{m,n}}{m^s}. \end{aligned}$$

楕円曲線 E_n の L 関数と E_1 の L 関数との関係を述べる. n を固定し, $2n$ と互いに素な m に対してヤコビ記号 $\left(\frac{n}{m}\right)$ で定まる $\mathbb{Z}$ 上の乗法的写像を χ_n と書くと

$$\begin{aligned} L(E_n, s) &:= \sum_{m=1}^{\infty} \frac{\chi_n(m) b_{m,1}}{m^s} \\ &= 1 - 2\left(\frac{n}{5}\right) 5^{-s} - 3\left(\frac{n}{3}\right)^2 9^{-s} + 6\left(\frac{n}{13}\right) 13^{-s} + \cdots \end{aligned}$$

となることがわかる [4, p.81]. $L(E_n, s)$ は $L(E_1, s)$ の指標 χ のツイストといい, $L(E_n, s) = L(E_1, \chi_n, s)$ と書く.

また, 保型形式 $f(z) = \sum_{n=0}^{\infty} d(n) q^n$ に対して, その L 関数を

$$L(f, s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s} \tag{3.23}$$

と定義する. $L(f, s)$ は整関数に解析接続されることが知られている. さらに

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right) \Gamma(s) L(f, s) \tag{3.24}$$

とおくと

$$\Lambda(s) = C\Lambda(k - s)\ (C = \pm 1) \tag{3.25}$$

という関数等式を満たすことが知られている.

Weil の定理を解説する. 大雑把に述べると, ディリクレ級数 $\sum d(n)n^{-s}$ の十分多くのツイスト $\sum \chi(n)d(n)n^{-s}$ がある関数等式を持つとき, 対応する q 展開が $M_k(\Gamma_0(N))$ に入るという主張である.

χ_0 を N を法とする固定したディリクレ指標とする. χ をコンダクター m のディリクレ指標で, m は N を割らない奇素数, または 4 となるものを走るとする. 注意として, m の値のなす十分大きな集合といえば, その集合が任意に与えられた数列 $\{u+jv\}_{j\in\mathbb{Z}}$, $(u,v)=1$ の元 m を少なくとも 1 つは含むことを表すとする. ディリクレの算術級数定理より, 任意のそのような等差数列は素数を含むことがわかる. また, 指標 χ のなす十分大きな集合といえば, m が十分大きな集合を動くときのコンダクターが m となるすべての指標 χ のなす集合を表すとする.

コンダクター m の任意の指標 χ に対して次の様におく.

$$C_\chi = C\chi_0(m)\chi(N)g(\chi)/g(\bar{\chi}). \tag{3.26}$$

ここで, $g(\chi) = \sum_{j=1}^{m} \chi(j)e^{(2\pi ij)}$ はガウス和である. 与えられた q 展開 $f(z) = \sum_{n=0}^{\infty} d(n)q^n$ が $|d(n)| = O(n^c)$ を満たすとき, $L(f,s)$ を (3.23) で定め, $\Lambda(s)$ を (3.24) で定める. また, 次の様に定める.

$$L(f,\chi,s) = \sum_{n=1}^{\infty} \chi(n)d(n)n^{-s}, \tag{3.27}$$

$$\Lambda(\chi,s) = (m\sqrt{N}/2\pi)^s\Gamma(s)L(f,\chi,s). \tag{3.28}$$

このとき, 次の定理が知られている.

定理 3.29 (Weil の定理 [4, p.143]). コンダクター m の指標 χ のなす十分大きな集合に対して, (3.28) で定義される $\Lambda(\chi,s)$ は任意の垂直な帯状領域で有界な整関数に拡張され, (3.27) で定義される C_χ により関数等式 $\Lambda(\chi,s) = C_\chi\Lambda(\bar{\chi},k-s)$ を満たすと仮定する. このとき,

$$f \in M_k(N,\chi_0).$$

さらに $L(f,s)$ がある $\epsilon > 0$ に対して $\mathrm{Im}\ s > k-\epsilon$ で絶対収束するならば f はカスプ形式となる.

Weil の定理を用いると次がわかる.

$$L(E_1,s) = 1 - 2\cdot 5^{-s} - 3\cdot 9^{-s} + 6\cdot 13^{-s} + \sum_{m\geq 17} \frac{b_{m,n}}{m^s}$$

に対応する q 展開

$$f_{E_1}(z) := q - 2q^5 - 3q^9 + 6q^{13} + \sum_{m\geq 25} b_{m,1}q^m$$

は重さ 2, レベル 32 のカスプ形式になる [4].

一般に, 虚数乗法をもつ任意の楕円曲線の L 関数に対して, 対応する q 展開は重さ 2 の保型形式となることが示される [4]. 虚数乗法を持たない楕円曲線の多くもこの性質を満たすことが知られていたが, $\mathbb{Q}$ 上の任意の楕円曲線に対しても成り立つことが示された [18].

楕円曲線の L 関数とランクとの関係について触れる.

定理 3.30 (Coates-Wiles [3]). *E を虚数乗法を持つ楕円曲線とする. このとき, E のランクは 0 より大きいならば $L(E,1)=0$ である.*

また, 虚数乗法を持つ楕円曲線 E に対して, $L(E,s)$ の $s=1$ での零点の位数が 0 または 1 ならば, その零点の位数はランクと一致することが示された [4]. その後, Kolyvagin によりモジュラー楕円曲線という広い楕円曲線のクラスに対し同じ定理が成り立つことが示された [6, 7, 10].

3.3 主定理の紹介と証明

この章では Tunnell による主定理の紹介と証明を与えていくことにする. t を正の整数とし, z を複素上半平面の元で $q = e^{2\pi iz}$ とする. テータ関数 $\theta_t(z)$ を $\theta_t(z) = \sum_{-\infty}^{\infty} q^{tm^2}$ とする. $\theta_t(z)$ は重さ 1/2, レベル 128, 指標 χ_t による保型形式となる. Serre-Stark [11] の結果より $\{\theta_2(z), \theta_8(z), \theta_{32}(z)\}$ は重さ 1/2, レベル 128 のモジュラー形式の基底となり, $\{\theta_1(z), \theta_4(z), \theta_{16}(z)\}$ は重さ 1/2, レベル 128, 指標 χ_2 の保型形式の基底となる.

$g(z) = q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})$ とする. $g(z)$ は重さ 1, レベル 32, 指標 χ_2 の正規化された唯一の newform である (定理 3.32). さらに, $\{g(z)\theta_2(z), g(z)\theta_8(z), g(z)\theta_{32}(z)\}$ は重さ 3/2, レベル 128 のカスプ形式の基底となり, $\{g(z)\theta_1(z), g(z)\theta_4(z), g(z)\theta_{16}(z)\}$ は重さ 1/2, レベル 128, 指標 χ_2 のカスプ形式の基底となる. Tunnell は $L(E_1, s)$ に対応する $f_{E_1} \in S_2(\tilde{\Gamma}_0(32))$ に志村対応で写る $f \in S_{3/2}(\tilde{\Gamma}_0(N), \chi)$ をすべて求めた (定理 3.33). Niwa [9] により $\mathrm{SH}(f)$ は $S_2(\tilde{\Gamma}_0(N/2), \chi^2)$ の元となることが知られている. よって, $N = 64$ と取りたい. しかし, $\mathrm{SH}(f)$ が $N/2$ の真の約数 N' に対して, $S_2(\tilde{\Gamma}_0(N'), \chi^2)$ に入るかもしれない. Tunnell は f_{E_1} に写るような, レベル 64 の f はなく, f_{E_1} の志村対応による逆像は少なくともレベル 128 を持つことを計算で示した.

志村対応と L 関数との関係を結びつける Waldspurger の定理を紹介する. Tunnell はこの定理を結びつけることにより主定理 3.34 を示した.

定理 3.31 (Waldspurger [17]). ϕ を重さ $k-1$, 指標 χ^2 による newform で, 重さ $k/2$ の保型形式 f の志村対応のもとでの像とする. ϕ のレベルは 16 で割り切れるものとする. このとき, 平方因子を持たない整数から複素数 $\mathbb{C}$ への次の様な関数 $A(t)$ が存在する. ここで, n^{sf} と書いたら平方因子を持たない自然数とする.

1. $A(t)^2\epsilon(\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, 1/2) = 2(2\pi)^{(1-k)/2}\Gamma((k-1)/2)L(\phi, \chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, (k-1)/2)$.
2. 任意の正の整数 N に対して,$\sum A(n^{sf})c(n)q^n$ により生成される重さ $k/2$, レベル N, 指標 χ の空間が志村対応による ϕ の逆像に一致するような, ある具体的に書ける関数 $c(n)$ の有限集合が存在する

論文 [17] ではより一般的な形で述べられているがここでは主定理 3.34 の証明に必要な形で書き表している. Hecke 指標 η に対して定まる因子 $\epsilon(\eta, 1/2)$ とは [15] で述べられているものであり, 2 次指標に対しては値が 0 となるものである. 具体的に記述できる $c(n)$ は論文 [17] で 11 通り与えられている.

定理 3.32 (Tunnell [16]). $g(z)$ は重さ 1, レベル 32, 指標 χ_2 であり, 正規化された唯一の newform である.

$$g(z) = \sum(-1)^{m+n}q^{(4m+1)^2+16n^2} = \sum(-1)^n q^{(4m+1)^2+8n^2}.$$

ここで $g(z)$ の 2 通りの表現はすでに得られている結果である (Moreno [8]).

定理 3.33 (**Tunnell [16]**)**.** 重さ 3/2 のカスプ形式 $g(z)\theta_2, g(z)\theta_4, g(z)\theta_8, g(z)\theta_{16}$ は志村対応により, 重さ 2, レベル 32 のカスプ形式 f_{E_1} に写る.

証明. $\{g(z)\theta_2(z), g(z)\theta_8(z), g(z)\theta_{32}(z)\}$ は重さ 3/2, レベル 128 のカスプ形式の基底であった. これらの q 展開の形は

$$\begin{aligned} g(z)\theta_2(z) &= q + 2q^3 + q^9 - 2q^{11} - 4q^{17} - 2q^{19} - 3q^{25} + 4q^{33} - 4q^{35} + \cdots \\ g(z)\theta_8(z) &= q + q^9 - 4q^{17} - 3q^{25} + 4q^{33} + \cdots \\ g(z)\theta_{32}(z) &= q - q^9 - 2q^{17} + q^{25} + 2q^{33} + \cdots \end{aligned}$$

である. Hecke 作用素 T_{p^2} は重さ 3/2, レベル 128 のカスプ形式を同じく重さ 3/2, レベル 128 のカスプ形式に写す. T_{3^2}, T_{5^2} を考えると $g(z)\theta_2(z), g(z)\theta_8(z), 2g(z)\theta_{32}(z) - g(z)\theta_8$ は固有形式であり, 始めの 2 つの固有値は $\lambda_3 = 0$, $\lambda_5 = -2$ である. また, $2g(z)\theta_{32}(z) - g(z)\theta_8 = \sum_{m=-\infty}^{\infty} \psi(m) m q^{m^2}$ と書ける. ここで ψ は非自明なコンダクター 4 の 2 次指標である.

任意の T_{p^2} に対して $g(z)\theta_2(z), g(z)\theta_8(z)$ が固有形式であることを得たい. $g(z)\theta_2(z), g(z)\theta_8(z)$ と $\sum_{m=-\infty}^{\infty} \psi(m) m q^{m^2}$ の T_{3^2}, T_{5^2} の固有値が一致しないので, 直交することがわかる. ゆえに, $g(z)\theta_2(z), g(z)\theta_8(z)$ の空間は T_{p^2} で不変である. $g(z)(\theta_2(z) - \theta_8(z))$ の n 番目の係数は n が 8 を法として 3 と合同のとき 0 ではなく, $g(z)\theta_8(z)$ の n 番目の係数は 8 を法として 1 と合同のとき 0 ではない. 命題 2.16 より $T_{p^2}(g(z)(\theta_2(z) - \theta_8(z)))$ と $T_{p^2}(g(z)\theta_8(z))$ との n 番目の q 展開係数が 0 となっていない係数番号は 8 を法として一致している. T_{p^2} は $g(z)(\theta_2(z) - \theta_8(z)), g(z)\theta_8(z)$ の張る空間に作用しているので, それらは任意の T_{p^2} に対する一次独立な固有形式である.

志村対応によりレベルが少なくとも 128 である ϕ_1, ϕ_2 が存在する. $p = 3, 5$ の固有値がわかっているので [1, Table 3] より $\phi_1 = \phi_2 = f_{E_1}$ である. $g(z)\theta_4(z), g(z)\theta_{16}$ の場合はこのアナロジーである.

□

定理 3.34 (**Tunnell [16]**)**.** $z \in \mathbb{H}, q = e^{2\pi i z}$, $g(z) = q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})$, $\theta_t(z) = \sum_{n=-\infty}^{\infty} q^{tn^2}$, $(t \in \mathbb{Z}_{>0})$ として,
$g(z)\theta_2(z)$, $g(z)\theta_4(z)$ の q 展開を次のようにおく.

$$g(z)\theta_2(z) = \sum_{n=1}^{\infty} a(n) q^n, \quad g(z)\theta_4(z) = \sum_{n=1}^{\infty} b(n) q^n.$$

n を平方因子を持たない奇数とする. このとき,

$$L(E_n, 1) = \frac{a(n)^2 \beta n^{-\frac{1}{2}}}{4}, \quad L(E_{2n}, 1) = \frac{b(n)^2 \beta (2n)^{-\frac{1}{2}}}{2}.$$

ただし, $\beta = \displaystyle\int_1^{\infty} \frac{dx}{\sqrt{x^3 - x}} = 2.62205\cdots$ である.

証明. Waldspurger の定理 [17] より, 次の 2 つの条件を満たす, 平方因子を持たない自然数から $\mathbb{C}$ への関数 $A(t)$ が存在する.

1. $A(t)^2 = L(f_{E_1}, \chi_t, 1)(= L(E_t, 1))$.
2. 具体的にかける関数 $c(n)$ の有限集合で $c(n)$ に対して $\sum A(n)c(n)q^n$ の集合の張る空間が重さ $3/2$, レベル 128, $\mathrm{SH}(f) = f_{E_1}$ となる f の集合と一致するものが存在する.

ここで, $c(n) = n^{\frac{1}{4}} \prod c_p(n)$, p は奇数, n は平方因子を持たないものに対して $c_p(n) = 1$ となるものである. つまり平方因子を持たない n に対し $c(n) = n^{\frac{1}{4}} c_2(n)$ となる. ここで, $c_2(n)$ は 8 を法として奇数となる n により定まる定数である.

χ が自明な場合についてみていく. $g(z)\theta_2(z)$, $g(z)\theta_8(z)$ は重さ $3/2$, レベル 128, $\mathrm{SH}(f) = f_{E_1}$ となる任意の T_{p^2} に関する一次独立な固有形式からなる極大系であった.

$g(z)\theta_2(z)$, $g(z)\theta_8(z)$ の q 展開の形は $n \not\equiv 1, 3 \mod 8$ での係数は 0 ではない. つまり, $n \equiv 5, 7 \mod 8$ に対して $A(n) = 0$ となる. $c(n)$ を $a(n) = \beta_1 A(n) n^{\frac{1}{4}}$, $a(n) = \beta_3 A(n) n^{\frac{1}{4}}$ となるそれぞれ $n \equiv 1, 3 \mod 8$ で定まる定数 β_1, β_3 とする. 両辺 2 乗すれば次のようになる,

$$\begin{aligned}
&a(n)^2 = \beta_1^2 L(E_n, 1) n^{\frac{1}{2}} && n \equiv 1 \mod 8,\\
&a(n)^2 = \beta_3^2 L(E_n, 1) n^{\frac{1}{2}} && n \equiv 3 \mod 8,\\
&a(n)^2 = 0 = A(n)^2 = L(E_n, 1) && n \equiv 5, 7 \mod 8.
\end{aligned}$$

β_1, β_3 を計算する.

$$\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.62205\cdots$$

とする. BSD [2] より

$$\frac{L(E_1, 1)}{\beta} = \frac{1}{4}, \quad \frac{L(E_3, 1) 3^{\frac{1}{2}}}{\beta} = 1.$$

また $a(1) = 1$, $a(3) = 2$ より

$$1 = \beta_1^2 L(E_1, 1), \quad 4 = \beta_3^2 L(E_3, 1) 3^{\frac{1}{2}}.$$

よって

$$\frac{4}{\beta} = \beta_1^2 = \beta_3^2.$$

ゆえに

$$L(E_n, 1) = \frac{a(n)^2 n^{-\frac{1}{2}} \beta}{4}.$$

$\chi = \chi_2$ の場合についてみていく. Waldspurger [17] の定理を用いると

$$A(t)^2 = L(f_{E_1}, \chi_2 \chi_t, 1) = L(E_{2t}, 1)$$

である. このとき基底は $(g(z)\theta_4(z) - g(z)\theta_{16}(z)), g(z)\theta_{16}(z)$ であるので, $n \equiv 3, 7 \mod 8$ に対して $A(n) = 0$ となる. $c(n)$ を $b(n) = \gamma_1 A(n) n^{\frac{1}{4}}$, $b(n) = \beta_5 A(n) n^{\frac{1}{4}}$ となるそれぞれ $n \equiv 1, 5 \mod 8$ で定まる定数 γ_1, γ_5 とする. 両辺 2 乗すれば次のようになる,

$$\begin{aligned} b(n)^2 &= \gamma_1^2 L(E_{2n}, 1) n^{\frac{1}{2}} && n \equiv 1 \mod 8, \\ b(n)^2 &= \gamma_5^2 L(E_{2n}, 1) n^{\frac{1}{2}} && n \equiv 5 \mod 8. \end{aligned}$$

γ_1, γ_5 を計算する.

$$\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.62205\cdots$$

とする. BSD [2] より

$$\frac{L(E_2, 1)}{\beta} = \frac{1}{2}, \quad \frac{L(E_{10}, 1) 5^{\frac{1}{2}}}{\beta} = 2.$$

また $b(1) = 1$, $b(3) = 2$ より

$$1 = \gamma_1^2 L(E_2, 1), \quad 4 = \gamma_5^2 L(E_{10}, 1) 5^{\frac{1}{2}}.$$

よって

$$\frac{2 \cdot 2^{\frac{1}{2}}}{\beta} = \gamma_1^2 = \gamma_5^2.$$

ゆえに

$$L(E_{2n}, 1) = \frac{b(n)^2 2 n^{-\frac{1}{2}} \beta}{2}.$$

□

$g(z)\theta_2(z)$ の q 展開は

$$g(z)\theta_2(z) = q + 2q^3 + q^9 - 2q^{11} - 4q^{17} - 2q^{19} - 3q^{25} + 4q^{33} - 4q^{35} + \cdots$$

となっている. Tunnell の定理より, 平方因子を持たない奇数番目の係数が 0 となっていない $\mathbf{1}, \mathbf{3}, \mathbf{11}, \mathbf{17}, \mathbf{19}, \mathbf{33}, \mathbf{35}$ は合同数ではないことがわかる. また, 平方因子を持たない奇数番目の係数が 0 となっている $\mathbf{5}, \mathbf{7}, \mathbf{13}, \mathbf{15}, \mathbf{21}, \mathbf{23}, \mathbf{29}, \mathbf{31}$ は合同数の可能性がある. 弱 BSD 予想が成り立てばこれらは合同数であることがわかる.

しかし, 弱 BSD 予想を認めなくても小さい数で計算により確かめることも可能なものもある. 平方因子を持たない n に対して

$$X^2 + Y^2 = Z^2, \quad \frac{XY}{2} = n \tag{3.35}$$

を満たす有理数解 (X, Y, Z) を求めればよい. $\mathbf{5}, \mathbf{7}, \mathbf{13}, \mathbf{15}, \mathbf{21}, \mathbf{23}, \mathbf{29}, \mathbf{31}$ が実際にどのような直角三角形の面積になっているか表でみる.

	(X,Y,Z)
5	$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$
13	$\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$
15	$\left(\frac{15}{2}, 4, \frac{17}{2}\right)$
21	$\left(\frac{7}{2}, 12, \frac{25}{2}\right)$
23	$\left(\frac{80155}{20748}, \frac{41496}{3485}, \frac{905141617}{72306780}\right)$
29	$\left(\frac{99}{910}, \frac{52780}{99}, \frac{48029801}{90090}\right)$
31	$\left(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}\right)$

$5, 15, 21$ は比較的, 有理数解 (X, Y, Z) を見つけ易いが小さい数でも見つけ難いものもある. これは 2 つの関係式 (3.35) の解となる有理数の組の可能性が無限通りあるからである.

3.4 q 展開の n 番目の係数との関連

最後に **Introduction** で述べた, Tunnell の定理 3.34 と実際の q 展開の n 番目の係数との関連について述べる.
$g(z)$ は

$$g(z) = (\theta_1(z) - \theta_4(z))(\theta_{32}(z) - \frac{1}{2}\theta_8(z))$$

と書けるので,

$$g(z)\theta_2(z) = (\theta_1(z) - \theta_4(z))(\theta_{32}(z) - \frac{1}{2}\theta_8(z))\theta_2(z)$$

となる. いまは奇数 n に対して, $g(z)\theta_2(z)$ の n 番目に興味がある. それは次の n 番目の係数と等しくなる.

$$\theta_1(z)(\theta_{32}(z) - \frac{1}{2}\theta_8(z))\theta_2(z) = \sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+8z^2}.$$

n 番目の係数が 0 となるのは

$$\#\{x,y,z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\}$$

となるときである. 偶数 n に対しては $g(z)\theta_4(z)$ の n 番目を調べてやればよい. それは次の n 番目の係数と等しくなる.

$$\theta_1(z)(\theta_{32}(z) - \frac{1}{2}\theta_8(z))\theta_4(z) = \sum_{x,y,z\in\mathbb{Z}} q^{4x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} q^{4x^2+y^2+8z^2}.$$

この場合 n 番目の係数が 0 となるのは

$$\#\{x,y,z \in \mathbb{Z} | \frac{n}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} | \frac{n}{2} = 2x^2 + y^2 + 8z^2\}$$

となるときである.

参考文献

[1] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV*. Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin, 1975.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, Vol. 218, pp. 79–108, 1965.

[3] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, Vol. 39, No. 3, pp. 223–251, 1977.

[4] Neal Koblitz. *Introduction to elliptic curves and modular forms*, Vol. 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[5] Winfried Kohnen. Modular forms of half-integral weight on $\Gamma_0(4)$. *Math. Ann.*, Vol. 248, No. 3, pp. 249–266, 1980.

[6] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, Vol. 52, No. 3, pp. 522–540, 670–671, 1988.

[7] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, Vol. 87 of *Progr. Math.*, pp. 435–483. Birkhäuser Boston, Boston, MA, 1990.

[8] Carlos J. Moreno. The higher reciprocity laws: an example. *J. Number Theory*, Vol. 12, No. 1, pp. 57–70, 1980.

[9] Shinji Niwa. Modular forms of half integral weight and the integral of certain theta-functions. *Nagoya Math. J.*, Vol. 56, pp. 147–161, 1975.

[10] Karl Rubin. The work of Kolyvagin on the arithmetic of elliptic curves. In *Arithmetic of complex manifolds (Erlangen, 1988)*, Vol. 1399 of *Lecture Notes in Math.*, pp. 128–136. Springer, Berlin, 1989.

[11] J.-P. Serre and H. M. Stark. Modular forms of weight 1/2. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pp. 27–67. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.

[12] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[13] Goro Shimura. Modular forms of half integral weight. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 57–74. Lecture Notes in Math., Vol. 320. Springer, Berlin, 1973.

[14] Joseph H. Silverman. *The arithmetic of elliptic curves*, Vol. 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[15] J. Tate. Number theoretic background. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pp. 3–26. Amer. Math. Soc., Providence, R.I., 1979.

[16] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, Vol. 72, No. 2, pp. 323–334, 1983.

[17] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, Vol. 60, No. 4, pp. 375–484, 1981.

[18] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, Vol. 141, No. 3, pp. 443–551, 1995.